AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of South Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

IINFORMATION ASSOCIATED WITH RBMUNN30@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, INC.,

Case No. 2:20-cr-598

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of South Carolina , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 545(a)	Importation of merchandise into the United States contrary to law
18 USC 922(g)(1)	Felon in possession of a firearm

The application is based on these facts:
See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Hailey Barraco
Applicant's signature

Hailey Barraco, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: July 13, 2020

Mary Gordon Baker
Judge's signature

City and state: Charleston, SC

Mary Gordon Baker, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH RBMUNN30@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, INC., HEADQUARTERED AT 1600 AMPHITHEATER PARKWAY MOUNTAIN VIEW, CA 94043, AND DEVICE CHROMEBOOK LENOVO LAPTOP, SERIAL NUMBER: LR05VGU6 AND DATA PREVIOUSLY EXTRACTED FROM RETURNED DEVICES SAMSUNG GALAXY NOTE 10+, ANDROID ID: A90FFD415DF00984, AND APPLE IPAD, SERIAL NUMBER: DMPVP6HPLJL	Case No. 2:20-cr-598

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Hailey Barraco, a Special Agent with Immigration and Customs Enforcement, Homeland Security Investigations ("ICE/HSI"), United States Department of Homeland Security, being first duly sworn, depose and state under oath as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for (1) information associated with the Google account RBMUNN30@GMAIL.COM (hereinafter "SUBJECT ACCOUNT"), (2) an electronic device owned and/or possessed by RAYMOND BRANDON MUNN (hereinafter "SUBJECT DEVICE"), and (3) data from two additional devices owned and/or possessed by RAYMOND BRANDON MUNN (hereinafter, "MUNN"),

HB

which were returned to him following extraction of the data they contained (hereinafter "EXTRACTED DATA").

2. Concerning the SUBJECT ACCOUNT, I make this affidavit in support of an application for a search warrant for information associated with the SUBJECT ACCOUNT that is stored at premises owned, maintained, controlled, or operated by Google Inc., an electronic communications service/remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google Inc., to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the account, including the contents of communications. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

3. Concerning the SUBJECT DEVICE, I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—a laptop computer—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

4. Concerning the EXTRACTED DATA, I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant

authorizing the search of the data described in Attachment B, which was previously extracted from devices described in Attachment A.

5. I am a Special Agent with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and have been so employed since April of 2019. I am currently assigned to the Assistant Special Agent in Charge (ASAC) Charleston, SC office. My responsibilities as a Special Agent include investigating crimes involving the importation and exportation of merchandise contrary to law, controlled substances, and child exploitation. I am a graduate of the Federal Law Enforcement Training Center and the HSI Special Agent Training Academy.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF SUBJECT ACCOUNT, SUBJECT DEVICE, AND EXTRACTED DATA

7. The SUBJECT ACCOUNT to be searched is information associated with RBMUNN30@GMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Google Inc.

8. The SUBJECT DEVICE to be searched is a Chromebook Lenovo Laptop, serial number: LR05VGU6. The Chromebook Lenovo Laptop is currently located in the evidence locker at 3950 Faber Place Drive, 3rd Floor, N. Charleston, SC 29405.

9. The EXTRACTED DATA to be searched is data that was extracted by consent of MUNN from the following devices at the scene of a search warrant executed on the residence of MUNN:

a. Samsung Galaxy Note 10+, Android ID: a90ffd415df00984, and

b. Apple Ipad, serial number: DMPVP6HPLJL.

Following extraction of the data from the Samsung Galaxy Note 10+ and Apple Ipad, these devices were returned to MUNN.[1]

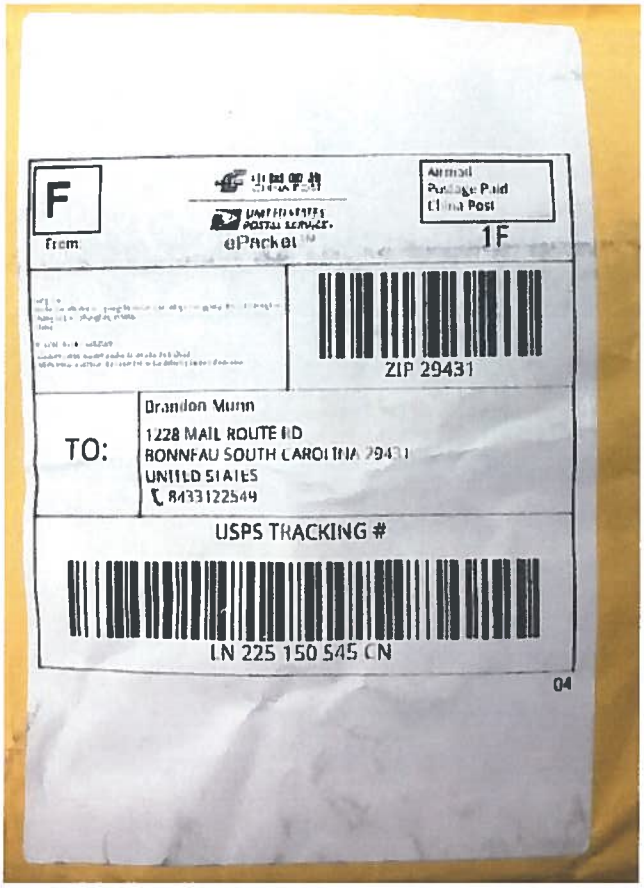
10. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 United States Code Sections 545(a) and 922(g)(1) have been committed by RAYMOND BRANDON MUNN. There is also probable cause to search the SUBJECT ACCOUNT, SUBJECT DEVICE, and EXTRACTED DATA described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B. The warrant will be executed in accordance with Attachment C.

C. Probable Cause

11. On April 10, 2020, a United States Postal Service Mail Parcel, arrived at the JFK Mail Facility, tracking #: LN225150545CN, originating from Zhu Long, Shanghai No. 18 South District Jiangchuan Second Village S, Shanghai, 315800 China. The parcel was found to contain a firearm silencer and was labeled on the outside as a "fuel filter."

[1] MUNN has since obtained legal counsel who has asked that the devices obtained by consent not be searched at this time. Although the EXTRACTED DATA and SUBJECT DEVICE were already in the custody of law enforcement at the time of Defense Counsel's request, the undersigned seeks a search warrant out of an abundance of caution.

12. On April 23, 2020, HSI Charleston was notified of the interception and accepted it for further investigation of the party to whom it was addressed, who was identified as RAYMOND BRANDON MUNN of 1228 Mail Route Road, Bonneau, S.C. 29431. On May 6, 2020, HSI SA Hailey Barraco received the intercepted parcel. A photo of the shipping label on the parcel is provided below:



The estimated value of the firearm silencer is $99.00.

13. On May 8, 2020, images of the silencer were sent to the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), which was able to confirm the item seized was a firearm silencer. On May 13, 2020, a search of MUNN in the National Firearm Registration and

Transfer Record yielded no records, indicating that MUNN does not have the proper license or authority to receive a firearm silencer.

14. MUNN'S address of record with the South Carolina Department of Motor Vehicles (SCDMV) is 1228 Mail Route Road, Bonneau, S.C. According to SCDMV, KELLIE WHITE also resides at this residence. Berkeley County Property Records indicate WHITE as the owner of the 1228 Mail Route Road, Bonneau, S.C.

15. Listed on the parcel that contained the firearm silencer, was a phone number (843) 312-2549. Verizon Wireless records indicate subscriber information for (843) 312-2549 belongs to RAYMOND B. MUNN at 1228 Mail Route Road, Bonneau, SC. Records indicate the phone number has been active since March 18, 2009. Records also indicate this phone has access to a wireless hotspot and internet connection from mobile data.

16. According to the National Crime Information Center (NCIC) and the Charleston County Clerk of Court, MUNN was convicted on felony charges in connection with drug distribution in September 1996. Records also revealed MUNN was convicted for unlawful carrying of a firearm in August 2002.

17. On June 25, 2020, a federal search warrant was executed at 1228 Mail Route Road, Bonneau, SC 29431. The search warrant yielded the seizure of four handguns, a short barrel rifle (SBR), an SBR conversion kit, ammunition, firearm magazines, and a laptop. MUNN provided agents with written consent to search his electronic devices, which included his cell phone, tablet, and laptops. MUNN also provided written consent to search his Google Account: RBMUNN30@GMAIL.COM. Your Affiant and a computer forensic analyst confirmed the email address and password provided by MUNN were correct and changed the password so agents could review the email communication. MUNN's cell phone and Apple iPad were

returned to him as the forensic computer analyst was able to retrieve the data, EXTRACTED DATA, from these two devices while MUNN was being interviewed. After agents left the residence, it appears that MUNN changed the password to his Google account associated with RBMUNN30@GMAIL.COM, preventing agents from accessing the digital communications stored in this account.

18. During the interview, MUNN acknowledged the firearm silencer, which he claimed was a fuel filter, was purchased and paid for online via wish.com. While at MUNN'S residence, you affiant asked MUNN for consent to search his email account. MUNN indicated his email address was RBMUNN30@GMAIL.COM and provided your affiant with the password. According to wish.com, in order to sign up or log in, users are required to use an email address and password. Your affiant believes the google account MUNN provided written consent for was used to create the wish.com account. Your affiant also believes confirmation or receipt of the order on wish.com was sent to RBMUNN30@GMAIL.COM.

19. During the interview, MUNN was asked about the firearm silencer, which he indicated was fake, and he claimed that he purchased the item as a fuel filter for his motorcycle. After the interview, agents and MUNN went back to his residence where his motorcycle was located. When agents asked MUNN where on the motorcycle the fuel filter would be installed, MUNN was not able to indicate to agents where the item would go and how it would work.

20. During the interview, MUNN acknowledged he was aware felons were prohibited from owning or possessing a firearm, but claimed that he was not aware he was a felon. MUNN explained that he took a plea deal for 18 months probation for the distribution charge in 1996 and claimed his attorney did not explain to him that he was a felon.

21. During the interview, MUNN informed agents that he purchased the rifle found at his residence from Palmetto State Armory and claimed that he accurately filled out the paperwork necessary to complete the purchase. However, records from an ATF trace indicate the rifle was actually purchased by David Strickland in November 2014 from Palmetto State Armory.

TECHNICAL BACKGROUND

22. In my training, experience and investigation in this case, I have learned the following about Google:

a. Google, located at 1600 Amphitheatre Parkway in Mountain View, California, operates an email service known as "Gmail" through its web site at www.google.com, which is available free of charge to Internet users. Subscribers obtain an account by registering on the Internet with Google. Google asks subscribers to provide basic information such as name, zip code and other personal/biographical information; however, Google does not verify the information provided. Once Google email subscribers have completed their registration process, they may access their email accounts on servers maintained and/or owned by Google from any computer connected to the Internet located anywhere in the world;

b. Google maintains electronic records, including opened and unopened email pertaining to their subscribers, including account access information, email transaction information, and account application information;

c. Any email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by Google. The message can remain on Google's servers indefinitely if

the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically;

d. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination, usually to the email provider of the email addressee. Google's users have the option of saving a copy of the email sent. If the sender does so, the email can remain on Google's system indefinitely. A sender can delete a previously sent and stored email message, thereby eliminating it from the sender's "Sent" box maintained at Google, but if the recipient of that same message is a Google email subscriber, the message will remain in the recipient's "Inbox" until the recipient deletes it or unless the recipient's account is subject to account size limitations;

e. A Google subscriber can store files, including emails and image files, on servers maintained and/or owned by Google; and

f. Google offers its email subscribers the opportunity to access their accounts through a personalized or "home" web page, known as an "iGoogle" page. Subscribers can configure their "iGoogle" pages to display pre-set fields of information offered by Google or affiliated vendors. These fields of information include regional or specialized news headlines, localized weather reports, specific team scores, select stock prices, airfares to select travel destinations, specific job listings, and maps.

23. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable

storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

d. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

25. Based on my training, experience, and research, I know that many electronic devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS, PDA, and tablet. Such electronic devices have access to the internet therefore are assigned an IP address. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. There is probable cause to believe that things that were once stored on the electronic device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the electronic devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the electronic devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review

team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

31. Based on the forgoing, I request that the Court issue the proposed search warrant. There is reasonable cause to permit the execution of the requested warrant at any time in the day

or night because the execution may require technical resources and the assistance of Google, Inc. that may necessitate after hours retrieval.

Respectfully submitted,

Hailey Barraco
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on July 13, 2020

UNITED STATES MAGISTRATE JUDGE